Preprint of: Kirwan, G., Fullwood, C., & Rooney, B. (in press). Risk factors for social networking site scam victimisation amongst Malaysian students. *Cyberpsychology, Social Networking and Behavior*

Risk factors for Social Networking Site scam victimisation amongst Malaysian students

Grainne H. Kirwan[1], Chris Fullwood[2], Brendan Rooney[3]

[1] Department of Technology and Psychology, Dun Laoghaire Institute of Art, Design, and Technology, Dublin

[2] Institute of Psychology, University of Wolverhampton

[3] School of Psychology, University College Dublin

RUNNING TITLE: RISK FACTORS FOR SNS SCAM VICTIMISATION

Corresponding Author: Grainne H. Kirwan

Department of Technology and Psychology, Institute of Art, Design and Technology, Dun Laoghaire, Co Dublin, Republic of Ireland.

Grainne.kirwan@iadt.ie

Phone +3531 239 4724

Abstract

Social Networking Sites (SNS) can provide cybercriminals with various opportunities, including gathering of user data and login credentials to enable fraud, and the directing of users towards online locations which may install malware onto their devices. The techniques employed by such cybercriminals can include clickbait (text or video), advertisement of non-existent but potentially desirable products, and hoax competitions/giveaways. This study aimed to identify risk factors associated with falling victim to these malicious techniques. An online survey was completed of 295 Malaysian undergraduate students, finding that over one-third had fallen victim to SNS scams. Logistic regression analysis identified several victimisation risk factors including having higher scores in impulsivity (specifically cognitive complexity), using fewer devices for SNS, and having been on SNS for a longer duration. No reliable model was found for vulnerability to hoax valuable gift giveaways and 'friend view application' advertising specifically, but vulnerability to video clickbait was predicted by lower extraversion scores, higher levels of openness to experience, using fewer devices, and being on SNS for a longer duration. Other personality traits were not associated with either overall victimisation susceptibility, or increased risk of falling victim to the specific techniques. However, age approached significance within both the video clickbait and overall victimisation models. These findings suggest that Routine Activity Theory may be particularly beneficial in understanding and preventing SNS scam victimisation.

Keywords: Clickbait; Social Networking Sites; Fraud; Impulsivity; Cybercrime; Routine Activity Theory

Introduction

Social Networking Sites (SNS) have enabled a variety of frauds and scams[1-3]. Cybercriminals may gather login credentials and other confidential information by utilising various strategies to persuade users to share personal data[2]. These malicious techniques can include: 'clickbait' content promising highly entertaining videos or text; the advertising of special giveaways or competitions; and the advertising of desirable products, which are commonly in the form of applications which would permit users to know how frequently other specific users visit their profile pages, but in reality, no such application exists[2]. The specific techniques of the scam vary, for example malware might sometimes be installed on the user's device, while other times the cybercriminal may require the user to provide banking or personal data. In most cases the scam requires the user to knowingly or unknowingly provide the cybercriminal with access to their SNS account, which is then automatically used by the application software to further disseminate the malicious application, and may be used by the cybercriminal to gather additional data about the victim. In many cases the re-disseminated malicious application gives the appearance of being knowingly shared by the victim which may encourage contacts of the user to also fall victim to the scam as the content appears to have been endorsed by someone they know. The increased prevalence of these scams alongside the massive popularity of SNS necessitates the understanding of the risk factors associated with falling victim so that more effective strategies may be employed to protect users.

Agustina has argued for an increased focus on victimological perspectives for both understanding and preventing cybercrime[4]. An increasing number of articles have considered the victims of online fraud[5-7] although it must also be remembered that data collection methodologies may impact on the reliability of the data obtained from victims (e.g. the terminology used when describing the crime)[8], and so victim research must be conducted carefully. Nonetheless, certain factors have been

associated with higher risk of online fraud, such as being 'younger-old' (with an average age of late 60s), having a high level of education, and higher depression scores[9].

Some research has focused on the cognitive elements of victimisation, with scam susceptibility associated with poor decision-making, arising from both cognitive and motivational factors[10]. Overconfidence, which may arise due to confirmation bias[11], may be an example of a cognitive factor, while desire (for information, a product, or entertainment) may be an example of a motivation leading to engagement with online scams. Optimism bias[12] (or the tendency for one to underestimate the likelihood of negative outcomes) may also be a factor in victimisation – as Wiederhold notes, the potential of immediate gratification and optimism bias may encourage some individuals to engage in riskier decision making[13].

In addition to psychological and communication theories, criminological theories may also be of assistance in developing our understanding of why victimisation occurs. Routine Activity Theory[14] (RAT) is widely discussed in criminology, and describes how a criminal act requires three components to be simultaneously present: a motivated offender, a suitable target, and the absence of a capable guardian. The importance of RAT in understanding cybercrime has been identified for over fifteen years[15] and theories such as RAT have been applied to cybercrime victims[4]. Specifically, RAT has been applied to phishing victims in the Netherlands, but found no particular group which was more likely to be victimised, and no effect of anti-virus software as a guardian[16]. However, RAT may still be useful in understanding SNS victimisation as the likely offender may be 'present' for substantial durations of time due to automated software, while the more time that an individual spends on SNS, the more likely they are to come across such software and become a suitable target.

The personality traits of the five-factor model may provide some insights into victim proneness for SNS fraud and scams. Tendencies towards agreeableness and extraversion may heighten victimisation risk on SNS due to the inherent interactions with others. For example, Orchard and colleagues noted how extraverts were motivated to use SNS to make new connections, potentially opening them up to new sources of fraud[17]. Other factors such as neuroticism and conscientiousness may reduce victimisation risk[18], as heightened anxiety and attention to detail may result in a more security-conscious user. Another important personality trait related to fraud susceptibility may be impulsivity. Burgard and Schlembach suggest that fraud victimisation begins when a user experiences a reduction in levels of risk awareness and hence caution is diminished, permitting engagement with strangers[19]. Their perspective of the situation becomes unrealistic, and self-deceptive tendencies may emerge. Using the UPPS-R impulsivity scale, Whitty et al found that a lack of perseverance (but not pre-meditation, urgency, or sensation seeking) was associated with password sharing among professionals[20]. However, their study did not examine who these passwords were shared with – while it may be with fraudsters, it was possibly with friends and family.

Impulsivity is a complex construct. The 'Barratt Impulsiveness Scale 11' (BIS-11)[21] specifically identifies six first order factors, which can be combined into three second order factors and an overall impulsivity score. The second order factor of 'motor impulsiveness' comprises of the first order factors 'motor' and 'perseverance'. 'Motor' related characteristics include acting impulsively without thinking things through, being quick to come to decisions, spending beyond earnings, and being 'happy-go-lucky', while 'perseverance' is characterised by frequently changing jobs and/or residences and lack of future orientation. The second order factor of 'non-planning impulsiveness' is comprised of 'self-control' and 'cognitive complexity'. 'Self-control' is characterised by advance planning of tasks, excursions, and job security, while 'cognitive complexity' includes factors such as a

dislike of thinking about complex problems, high levels of boredom when solving thought problems, and disliking puzzle-solving. Finally, the second order factor of 'attentional impulsiveness' comprises of the first order factors 'attention' and 'cognitive stability'. 'Attention' considers factors relating to concentration and restlessness during lengthy events such as lectures or plays, while 'cognitive stability' relates to tendencies towards racing or extraneous thoughts. Based on these first-order dimensions and what we know about how SNS frauds operate, it is possible that the first order impulsivity factors of 'motor' and 'cognitive complexity' may provide the greatest indicators of victimisation risk, although other dimensions may also play a role and will be examined in this study. It should also be noted that the perseverance measure in the UPPS-R scale used by Whitty et al[20] is not directly comparable to the definition used in the BIS-11, with the UPPS-R scale focusing on traits which are more similar to the 'Attention' scale in the BIS-11.

The Current Study

As there is little previous literature regarding victimisation risk factors for online fraud, and even less relating to SNS scams in particular, the current research aims to further understanding of how SNS usage factors and personality might provide indicators of victimisation risk. The study seeks to identify if personality, impulsivity, SNS routine usage, and years using SNS are indicators of SNS scam victimisation.

Method

Participants

Participants were undergraduate students of a Malaysian university who completed the study for course credit (students were permitted to select from a range of research projects to fulfil the course credit requirement, and so were under no obligation to participate in this specific research).

Social media is very popular in Malaysia, with 73 percent of internet users accessing Facebook daily[22]. A total of 320 participants completed some of the study requirements, but 21 responses were deemed to be insufficiently complete to allow analysis, and a further four age-related outliers were removed (aged 27-40 years). The majority of respondents were female (n=218; 73.9%), and 21 years old (n=84; 28.5%) with age ranging from 18-26 years (mean = 21.29; sd = 1.572). Most participants were Chinese-Malaysian in ethnicity (n=132; 44.7%) with the second largest group indicating their ethnicity as Asian Chinese (n=80; 27.1%). Other Malaysian ethnicities comprised 19.3% of the sample (n=57). The remainder were from mixed or other ethnicities.

Age frequencies, participant routine usage and years of usage of SNS use are presented in Table 1. Most participants (n=259; 87.8%) used SNS on two or three different types of device (laptop, smartphone, tablet, eReader, etc.). The mean number of devices used was 2.45 (sd = 0.699).

Table 1: Participant age, routine usage and years of usage of social networking sites

	Frequency	**Percent**
Age		
18	5	1.7
19	31	10.6
20	53	18.1
21	84	28.7
22	65	22.2
23	34	11.6
24	7	2.4
25	10	3.4
26	4	1.4
Years using SNS		
1-3 years	5	1.7
4-5 years	52	17.8
More than 5 years	235	80.5
Routine Usage of SNS		
Less than once per week	2	.7
Several times per week	10	3.6
About once per day	15	5.3
Several times per day	105	37.4
About once per hour	32	11.4
Several times per hour	117	41.6

Materials

Social Networking Site Usage

Three questions examined general use of SNS, specifically regarding duration of use (years of usage), routine usage schedule (frequency of use), and devices utilised for SNS access.

SNS Fraud Victimisation

Awareness of SNS fraud was measured. Participants were presented with three different types of malicious SNS posts or apps and asked to indicate if they had seen such posts before, if they had guessed that it may have been a scam, and if they had fallen victim to the post (by clicking on it). Specifically, participants were asked about a) posts promoting applications which indicated that they would provide information about which of their friends frequently viewed the user's profile ('Friend Views App'); b) posts which suggested that those who followed their link would receive a valuable gift ('Valuable Gift App'); and c) posts which suggested that their friend had liked an especially outlandish or bizarre video and provided a link to that video ('Clickbait Video'). For each type of post participants were provided with images of real malicious posts of that genre gathered from social media as examples (three images were provided for each of the 'Friend Views App' and 'Clickbait Video' types, while two images were provided for the 'Valuable Gift App'). Participants were also encouraged to describe any other potential fraudulent post which they may have seen on SNS. These descriptions allowed the researchers to identify if the post identified by the participant was actually an SNS scam, or not. Where an SNS scam was detected by this description, the participant data was coded accordingly. Those who had fallen victim to any of these posts were asked further open-ended questions regarding their experiences.

Big Five Inventory (BFI-44)

The Big Five Inventory (BFI-44) is a 44-item inventory examining the big five personality dimensions[23-25]. Participants respond to each item on the inventory using a 5-point Likert scale from

'Disagree strongly' to 'Agree strongly'. This personality inventory has been widely used, demonstrating good validity and reliability[26].

Barratt Impulsiveness Scale (BIS-11)

The Barratt Impulsiveness Scale[21] (BIS-11) is a 30-item self-report inventory using a 4-point Likert scale ('Rarely/Never' to 'Almost Always/Always'). It includes six first order factors and three second order factors. This study utilises the first order factors as predictor variables in order to fully examine the range of facets in this trait[27]. The BIS-11 has also been widely used and found to be reliable across a wide range of populations[27].

Procedure

Participants completed the survey online. Informed consent was obtained and demographic information was collected. Further questions were presented in the order described in the Materials section. Following completion of the study the participants were provided with links to further information regarding online fraud.

Results

The majority of participants (n=177; 60.2%) had heard of SNS fraud, with 54 (18.4%) unsure if they had heard of it prior to the study. Over one-third of participants had fallen victim to one or more types of malicious post (n=100; 33.9%), with only 13 (4.4%) being unaware of having ever seen such a post or were unaware of its malicious nature. The frequency of victimisation of the sub-types of malicious posts is presented in Table 2. Most victims had only clicked on such posts once (n=51; 53.1%), although a substantial minority had clicked on such posts 2-3 times (n=40; 41.7%). Descriptive statistics for the BFI44 and the BIS11 are presented in Table 3.

Table 2: Victimisation of malicious posts on SNS

	Friend Views App	Valuable gift app	Clickbait video	Other potential scam
Seen and fell victim	28 (9.5%)	27 (9.2%)	76 (25.8%)	13 (4.4%)
Seen and did not click (identified it as a scam)	198 (67.1%)	199 (67.5%)	164 (55.6%)	110 (37.3%)
Seen and did not click (unaware it was a scam)	47 (15.9%)	38 (12.9%)	39 (13.2%)	21 (7.1%)
Never seen app	18 (6.1%)	23 (7.8%)	7 (2.4%)	51 (17.3%)
Unsure if ever seen app	4 (1.4%)	1 (0.3%)	5 (1.7%)	95 (32.2%)
Unanswered	0 (0.0%)	7 (2.4%)	4 (1.4%)	5 (1.7%)

Table 3: Descriptive statistics for BFI44 and BIS11

	Min.	Max.	Mean	SD
Extraversion	20	34	25.29	2.143
Agreeableness	22	35	28.18	2.207
Conscientiousness	21	35	27.49	2.490
Neuroticism	22	31	26.32	1.817
Openness	29	44	36.03	2.863
Attention	5	19	11.10	2.329
Cognitive Instability	3	12	7.12	1.835
Motor	8	28	14.86	3.365
Perseverance	4	13	7.46	1.755
Self-Control	6	24	13.45	3.302
Cognitive Complexity	6	17	11.69	2.118

A series of logistic regression analyses were conducted to determine the factors which successfully predict victimisation of SNS fraud enabling scams. Victimisation was recoded into 'Victimised' or 'Not victimised due to suspicion of a scam'. Other outcomes (lack of awareness of it being a scam, uncertainty regarding prior history, and lack of history of viewing this type of material) were removed from the analysis to permit clear distinction between those who had fallen victim to the scam and those who did not fall victim by identifying its malicious nature. Due to the exclusion of these outcomes, combined with missing values for some predictor variables, the number of cases varies in each analysis. Predictor variables examined were gender, age, length of time using SNS, routine usage of SNS, total number of devices used to access SNS, agreeableness, extraversion,

conscientiousness, neuroticism, openness to new experiences, and the 6 first level outputs of the BIS11 (attention, cognitive instability, motor, perseverance, self-control, cognitive complexity). The variables of length of time using SNS and routine usage of SNS were captured via nominal data and were recoded for analytic purposes into two categories each – fewer or more than 5 years of use, and less or more than hourly usage each day.

Using logistic regression analysis to identify factors influencing victimisation, the model could not significantly predict victimisation for 'friend views app' posts, (N=172, $\chi^2(16) = 17.198$, $p = .373$), 'valuable gift app' posts, (N=169, $\chi^2(16) = 22.609$, $p = .125$); or for other posts identified as scam by the participants (N=90, $\chi^2(16) = 20.815$, $p = .186$).

However, the model did significantly predict clickbait video victimisation (N=179, $\chi^2(16) = 40.522$, $p = .001$). The model accounted for between 20.3% and 28.4% of the variance in victimisation status, with 91.0% of non-victims successfully predicted. The victimised group were predicted with 47.4% accuracy. Overall accuracy of the model was 77.1%. Extraversion scores, openness to experience, total number of devices used for SNS and length of time using SNS reliability predicted victimisation (see Table 4). Age approached significance for prediction of victimisation (p = .058).

Table 4:

Logistic regression analysis predicting victimisation of video posts

	B	S.E.	Wald	Odds Ratio	95% C.I.	
					Lower	Upper
Age	.234	.123	3.585	1.263	.992	1.609
Total number of devices	-.904**	.295	9.408	.405	.227	.722
Extraversion	-.230*	.097	5.647	.794	.657	.960
Agreeableness	.053	.085	.382	1.054	.892	1.246
Conscientiousness	-.087	.087	1.002	.916	.773	1.087
Neuroticism	-.035	.102	.121	.965	.790	1.179
Openness	.148*	.074	4.022	1.159	1.003	1.339
Attention	-.130	.103	1.577	.878	.718	1.075
Cognitive Instability	.032	.117	.075	1.032	.821	1.297
Motor	.042	.074	.327	1.043	.902	1.206
Perseverance	.089	.125	.507	1.093	.856	1.395
Self-Control	.031	.070	.189	1.031	.898	1.184
Cognitive Complexity	.141	.110	1.655	1.151	.929	1.427
Gender	.541	.409	1.747	1.717	.770	3.827
SNS years of use[†]	-1.835**	.621	8.725	.160	.047	.539
Routine SNS use[†]	.631	.383	2.705	1.879	.886	3.984
Constant	-3.662	5.797	.399	.026		

*Significant at .05 level; **Significant at .01 level; [†]Parameter coding during logistic regression results in negative B value being associated with increased years of SNS usage/more frequent SNS routine usage.

Overall Victimisation

Victimisation of any type of deviant post was determined and utilised as the dependent variable. The full model significantly predicted victimisation (N=214, $\chi^2(16) = 36.068$, $p = .003$). The model accounted for between 15.5% and 21.6% of the variance in victimisation status, with 88.9% of non-victims successfully predicted. However, only 37.1% of predictions for the victimised group were accurate. Overall accuracy of the model was 72.0%. Total number of devices used for SNS, length of time using SNS, and cognitive complexity reliably predicted victimisation (see Table 5). Age approached significance for prediction of victimisation (p = .061).

Table 5:

Logistic regression analysis predicting victimisation of any deviant post

	B	S.E.	Wald	Odds Ratio	95% C.I.	
					Lower	Upper
Age	.203	.108	3.505	1.225	.991	1.516
Total number of devices	-.818***	.254	10.401	.441	.268	.725
Extraversion	-.138	.080	2.925	.871	.744	1.020
Agreeableness	.050	.075	.456	1.052	.908	1.218
Conscientiousness	-.008	.077	.012	.992	.853	1.152
Neuroticism	-.089	.089	1.002	.914	.768	1.089
Openness	.093	.063	2.180	1.098	.970	1.243
Attention	-.066	.087	.578	.936	.789	1.110
Cognitive Instability	-.027	.099	.073	.974	.801	1.183
Motor	.046	.061	.569	1.047	.929	1.180
Perseverance	.044	.111	.156	1.045	.840	1.299
Self-Control	.063	.062	1.008	1.065	.942	1.203
Cognitive Complexity	.207*	.094	4.835	1.230	1.023	1.480
Gender	.569	.369	2.380	1.766	.858	3.636
SNS years of use[†]	-1.353**	.478	8.000	.258	.101	.660
Routine SNS use[†]	.461	.340	1.845	1.586	.815	3.085
Constant	-5.403	5.253	1.058	.005		

*Significant at .05 level; **Significant at .01 level; ***Significant at .001 level; [†]Parameter coding during logistic regression results in negative B value being associated with increased years of SNS usage/more frequent SNS routine usage.

Repeat Victimisation

A logistic regression analysis was conducted to identify factors influencing repeat victimisation (i.e., where a victim had clicked on more than one malicious post vs. a single instance of victimisation). A total of 70 cases were included in this analysis. The model could not significantly predict repeat victimisation (N=70, $\chi^2(16) = 14.130$, $p = .589$).

Discussion

The results of the study indicate that more years of experience using SNS is associated with greater likelihood of falling victim to SNS scams. This finding is in line with the predictions based on Routine Activity Theory[14], with increased presence of an individual on SNS over time resulting in higher

victimisation risk. The low association between most impulsivity factors and victimisation was unexpected, although the findings were similar to those of previous research[20]. This may be indicative that the findings of Whitty et al[20] were not anomalous, and the connection between impulsivity and victimisation may be weaker than expected. Nevertheless, it was interesting to note that the trait of cognitive complexity was associated with increased risk and so it is possible that very specific facets of impulsivity may be helpful in predicting victimisation. The associations between introversion/ higher openness to experience and susceptibility to video type scams are of note, particularly as these associations were not noticed in the overall victimisation analysis. These associations, along with the results for age which approached significance for both the video posts and overall victimisation, are worthy of future investigation. As this study involved a relatively young sample it would be of particular interest to explore the potential influence of age with samples drawn from a wider range of age groups.

It is not clear why those who used fewer devices for SNS were more likely to experience victimisation. It is possible that certain types of malicious techniques are displayed more frequently on some platforms (e.g. desktop website versions) than others (e.g. smartphone apps). Further research should attempt to identify causes for this phenomenon. The Malaysian sample is derived from a collectivist-oriented culture[28], albeit one which has experienced greater influence from individualistic cultures in recent years. It would be of interest to conduct cross-cultural research to examine if these findings are also evident in individualistic cultures. It should also be noted that the participants in this study were all highly educated, attending undergraduate studies. Further research with a broader range of users should be completed.

Overall it would appear that there is no strong connection between social networking site scam victimisation and many personality traits and impulsivity factors, although it seems that the relative

predictive value of some traits varies according to the type of scam involved. This research has demonstrated the potential for Routine Activity Theory to be applied to SNS scams, which may provide opportunities for victimisation prevention, as well as identifying the role of SNS usage and cognitive complexity in potential victimisation.

Author Disclosure Statement

No competing financial interests exist

References

[1] Hatchimonji, G. (2014). 10 new social media scams to watch out for. Retrieved from CSO Online at http://www.csoonline.com/article/2457669/data-protection/data-protection-10-new-social-media-scams-to-watch-out-for.html

[2] Kirwan, G, Power, A. (2013). *Cybercrime: The Psychology of Online Offenders.* Cambridge: Cambridge University Press.

[3] Norton (n.d.). Top 5 Social Media Scams. Retrieved from https://ie.norton.com/yoursecurityresource/detail.jsp?aid=social_media_scams

[4] Agustina, JR. Understanding cyber victimisation: Digital architectures and the disinhibition effect. International Journal of Cyber Criminology 2015; 9: 35-54.

[5] Buchanan, T, Whitty, MT. The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law* 2014; 20:261-283.

[6] Cross, C. No laughing matter: Blaming the victim of online fraud. International Review of Victimology 2015: 21:187-204.

[7] Whitty, MT. Mass-marketing fraud: A growing concern. IEEE Security & Privacy 2015; 13:84-7.

[8]Beals, ME, Carr, DC, Mottola, GR, Deevy, MJ, Carstensen, LL. How Does Survey Context Impact Self-reported Fraud Victimization? The Gerontologist 2015, doi: 10.1093/geront/gnv082

[9]Lichtenberg, PA, Sugarman, MA, Paulson, D, Ficker, LJ, Rahman-Filipiak, A. Psychological and functional vulnerability predicts fraud cases in older adults: Results of a longitudinal study. Clinical Gerontologist 2015; 39:48-63.

[10]Lea, S, Fischer, P, Evans, K. (2009). The psychology of scams: Provoking and committing errors of judgement. A report for The Office of Fair Trading. Retrieved from UK Government Web Archive at http://webarchive.nationalarchives.gov.uk/20140402142426/http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf

[11]Nickerson, RS. Confirmation bias: A ubiquitous phenomenon in many guises. Review of general psychology 1998; 2: 175-220.

[12] Weinstein, ND. Unrealistic optimism about future life events. Journal of personality and social psychology 1980; 39:806-820.

[13] Wiederhold, BK. The role of psychology in enhancing cybersecurity. Cyberpsychology, Behavior, and Social Networking 2014; 17(3):131-2.

[14] Cohen, LE, Felson, M. Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review 1979; 44:588-608.

[15] Pease, K. (2001). Crime futures and foresight: Challenging criminal behaviour in the information age. In Wall DS, ed. *Crime and the Internet*. London/New York: Routledge, pp. 18-28.

[16] Leukfeldt, ER. Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking 2014; 17:551-5.

[17] Orchard L, Fullwood C, Galbraith N, Morris, N. Individual differences as predictors of social networking. Journal of Computer Mediated Communication 2014; 19:388-402.

[18] Tan FB, Sutherland, P. "Online consumer trust: a multi-dimensional model", Journal of Electronic Commerce in Organizations 2004; 2:40-58.

[19]Burgard, A, Schlembach, C. Frames of fraud: A qualitative analysis of the structure and process of victimisation on the internet. International Journal of Cyber Criminology 2013; 7: 112-124.

[20]Whitty, M, Doodson, J, Creese, S, Hodges, D. Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior, and Social Networking 2015; 18:3-7.

[21] Patton, JH, Stanford, MS, Barratt, ES. Factor structure of the Barratt Impulsiveness Scale. Journal of Clinical Psychology 1995; 6:768–774.

[22] Statistica (2016). Daily reach of leading social networks and mobile messenger apps in Malaysia as of July 2015. Retrieved from https://www.statista.com/statistics/496953/daily-active-users-of-leading-social-networks-malaysia/

[23] Benet-Martinez, V, John, OP. Los Cinco Grandes across cultures and ethnic groups: Multitrait multimethod analyses of the Big Five in Spanish and English. Journal of Personality and Social Psychology 1998; 75:729-750.

[24] John, OP, Naumann, LP, Soto, CJ. (2008). Paradigm Shift to the Integrative Big-Five Trait Taxonomy: History, Measurement, and Conceptual Issues. In John OP, Robins RW, Pervin LA, eds. *Handbook of personality: Theory and research.* New York, NY: Guilford Press, pp. 114-158.

[25] John, OP, Donahue, EM, Kentle, RL. (1991). The Big Five Inventory--Versions 4a and 54. Berkeley, CA: University of California, Berkeley, Institute of Personality and Social Research.

[26] John, OP, Srivastava, S. (1999). The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In Pervin LA, John OP, eds. *Handbook of personality: Theory and research (Vol. 2).* New York: Guilford Press, pp. 102–138.

[27] Stanford, MS, Mathias, CW, Dougherty, DM, Lake, SL, Anderson, NE, Patton, JH. Fifty years of the Barratt Impulsiveness Scale: An update and review. Personality and Individual Differences 2009; 47:385-395.

[28] Bochner, S. Cross-Cultural Differences in the self-concept a test of Hofstede's individualism/collectivism distinction. Journal of cross-cultural psychology 1994; 25:273-283.